(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 January 2003 (30.01.2003)

PCT

(10) International Publication Number
WO 03/009520 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US02/20697

(22) International Filing Date: 28 June 2002 (28.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/906,961 16 July 2001 (16.07.2001) US

(71) Applicant: AUTHENTIDATE HOLDING CORP. [US/US]; 2165 Technology Drive, Schenectady, NY 12308 (US).

(72) Inventor: BOTTI, John, T.; 325 Loudon Road, Loundonville, NY 12211 (US).

(74) Agent: RUEH, Mark; Clifford Chance Rogers & Wells LLP, 200 Park Avenue, New York, NY 10166 (US).

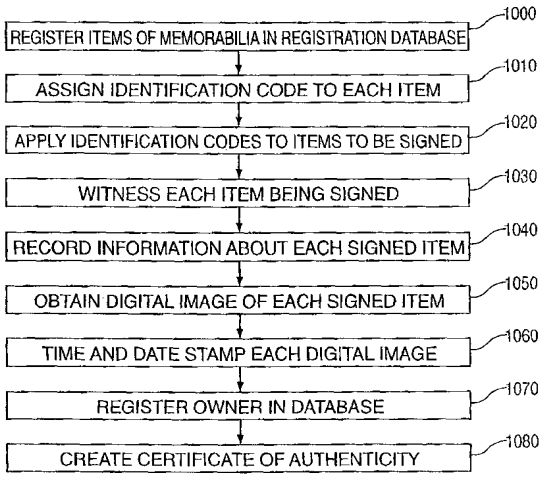
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD OF AUTHENTICATING MEMORABILIA



(57) Abstract: The system and method of authenticating an item of memorabilia (10) of the present invention provides an authenticating service that may authenticate and register an item of memorabilia (10) utilizing a digital imaging system to provide digital file authentication of the item by secure image marking. The system and method may include assigning an identification code (1010) to the item of memorabilia, recording a digital image of the item of memorabilia (1050), providing date and time information from a secure date and time reference, and marking the digital image of the item with date and time information (1060), a date/time value and an image value or assigning date and time information corresponding to the digital image according to the time the digital image was received or created. The item of memorabilia may be signed and witnessed by a third party (1030) and a digital image of the signed item and information may be processed and used to register the owner of the item (1070) and generate a certificate of authenticity of the signed item (1080).

WO 03/009520 A1

SYSTEM AND METHOD OF AUTHENTICATING MEMORABILIA

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority to United States Patent Application No. 09/906,961 filed on July 16, 2001, which is a continuation-in-part of United States Patent Application No. 09/562,735 filed on May 1, 2000.

FIELD OF THE INVENTION

This invention relates generally to digital imaging systems and more particularly to digital authentication of memorabilia.

BACKGROUND OF THE INVENTION

The market for U.S. collectibles dates back many years. For example, baseball cards depicting professional baseball players from various eras have long been collected, bought, sold and trade by enthusiasts since the early party of this century. Other areas of the sports collectibles market have developed over the years including memorabilia such as player uniforms, photographs, sporting equipment, ticket stubs, programs, souvenirs and numerous other items.

A major share of the collectibles market is represented by sports or entertainment memorabilia that is autographed by an athlete or other personality. Examples of autographed memorabilia are almost limitless and include autographed sports cards, jerseys, photographs, baseballs, football helmets and any piece of merchandise that can be signed. The extrinsic and intrinsic value of such autographed sports and entertainment memorabilia depends on many factors such as the prominence of the athlete or celebrity, the time when item was signed, the rarity of the autograph and, of course, the genuineness of the autograph. However, because of the high demand for autographed memorabilia and the difficulty in

assessing the genuineness of an autograph, there exists the problem of forgers and counterfeiters in the industry creating fraudulent autographs. The problem of fraud has diluted the value of genuine memorabilia and held back the growth of the sports memorabilia market. Thus, there has been a need for a system to detect and ensure the authenticity of an item of sports and entertainment memorabilia and, in particular, the authenticity of an autograph.

Various methods of authenticating memorabilia of various degrees of complexity have been developed in the collectibles industry though none have proved completely satisfactory to date. For example, less complex means of authenticating an autograph include providing the buyer with a certificate of authenticity stating that the signed item is genuine and providing a photograph of the item being signed with the certificate. Other methods include assigning the certificate of authenticity a number and dated description that is cataloged by the retailer of the signed memorabilia or creating a label corresponding to the certificate of authenticity that is affixed to the autographed item and recorded in a database by such retailer. A retailer may also issue a picture of the signing of the item that is filed by the authenticator with certificate information and registered. These techniques, however, are highly dependent on the reputation and honesty of the retailer or other authenticating party, do not adequately protect against counterfeit certificates of authenticity or adequately protect subsequent buyers of the item.

More complex techniques of authenticating the signed item include providing a certificate of authenticity with a numbered holograph label corresponding to the certificate of authenticity that is affixed to the item with a tamper-resistant seal and recorded in a database. As an additional step, invisible, permanent, infrared or ultraviolet activated ink mark corresponding to the hologram label may be used to tag the item. These techniques, however, are also highly dependent on the reputation and honesty of the retailer or authenticating party

and provide no means of verifying with a great degree of certainty the date the signed item can into existence. Additionally, these systems are often used by the manufacturer of the memorabilia and may be compromised by the vendor or the retailer.

Thus there is a need for a system of authenticating memorabilia that reduces the risk of fraud associated with the purchase of a signed item of memorabilia, that provides a subsequent purchaser of a signed item of memorabilia with assurance that the item is genuine, and that provides means to verify with great degree of certainty when the signed item came into existence or was first registered by the authenticating service provider.

SUMMARY AND OBJECTS OF THE INVENTION

The foregoing and other problems and deficiencies in authenticating memorabilia are solved and a technical advance is achieved by the present invention by combing a method of physically authenticating the item with a unique digital authentication system to provide digital file authentication of the item.

In various aspects, it is an object of the present invention to provide a system of authenticating memorabilia that reduces the risk of fraud associated with the purchase of a signed item of memorabilia. In various aspects, it is a further object of the present invention to provide a system of authenticating memorabilia that provides a subsequent purchaser of a signed item of memorabilia with assurance that the item is genuine. In various aspects, it is yet another object of the present invention to provide a system for authenticating memorabilia that can verify when the signed item of memorabilia came into existence or was first registered by the authenticating party.

A method employed in a system for authenticating memorabilia in one embodiment of the present invention comprises the steps of:

applying an identification code to an item of memorabilia

recording a digital image of the item of memorabilia

providing date and time information from a secure date and time reference;

generating a date/time value derived from said date and time reference;

generating an image value derived from said digital image;

marking said digital image with said date and time information, said date and time value and said image value; and

storing said marked digital image.

In accordance with other aspects of the invention, a method employed in a system for authenticating memorabilia in one embodiment of the present invention comprises the steps of:

applying an identification code to an item of memorabilia;

obtaining a handwritten signature on the item of memorabilia from a signor;

recording a digital image of the item of memorabilia;

providing date and time information from a secure date and time reference;

generating a date/time value derived from said date and time reference;

generating an image value derived from said digital image;

marking said digital image with said date and time information, said date/time value and said image value; and

storing said marked digital image

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other features and advantages of the present invention will become more apparent in light of the following detailed description of exemplary embodiments thereof, as illustrated in the accompanying drawings, where

Fig. 1 illustrates a system implementation for authenticating memorabilia according to one embodiment of the invention.

Fig. 2 is a flow chart illustrating the steps for authenticating memorabilia according to one embodiment of the invention.

Fig. 3 illustrates a sample certificate of authenticity used in one embodiment of the invention.

Fig. 4 illustrates a system implementation of one embodiment of the present invention utilizing a digital file management system;

Fig. 5 is a flow chart illustrating the file marking according to one embodiment of the present invention;

Fig. 6 is a flow chart illustrating validation of the CRCs in a filed marked image according to one embodiment of the present invention;

Fig. 7 is a flow chart illustrating calculation of the Image CRC for TIFF format images according to one embodiment of the present invention;

Fig. 8 is a flow chart illustrating calculation of the Date CRC for TIFF format images according to one embodiment of the present invention;

Fig. 9 is a flow chart illustrating calculation of the Image CRC for JPEG format images according to one embodiment of the present invention; and

Fig. 10 is a flow chart illustrating calculation of the Date CRC for JPEG format images according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates an exemplary embodiment of a system for authenticating memorabilia of the present invention. As shown in Figure 1, a central processor 110 is configured in communication with a first input device 40, a second input device 30, and a server 100 (described in more detail below) which includes or is connected to a secure time and date reference, a registration database 50, and output device 60. First input device 40 is adapted to input information associated with the item to be authenticated from the authenticating service provider and may comprise a personal computer, workstation,

keyboard or other input device. Second input device 30 is adapted to generate one or more digital image files associated with the item to be authenticated and may comprise a digital camera or a digital video recorder. An ID code is assigned to and applied on the surface of the item 10 of memorabilia to be signed and authenticated. The ID code may comprise a number identification code, a character based identification code, a bar code, a hologram or any other means of assigning a code or symbol of identification to the item to be signed. Item 10 may be a two-dimensional item of memorabilia such as a photo or sports card or a three-dimensional item of memorabilia such as a baseball or football helmet.

Figure 2 shows a flow diagram of one embodiment of the present invention. The flow diagram shows exemplary steps for a method of authenticating memorabilia for which an actual implementation could include only some of, as well as additional process steps. The method of authenticating memorabilia according to one embodiment of the present invention begins with a visual inspection of the items to be authenticated (e.g., baseballs, helmets, sports cards, etc.) at a particular sporting event or scheduled signing appearance. Detailed computer entries of all items to be signed are made and may be stored and registered in a master database 50 of the authenticating service provider or other third party. (Step 1000). In cases where more than one item will be signed, an inventory lot can be organized and numbered in series (e.g., as item 1 of 25, item 2 of 25, etc.). In addition, information about the manufacturer or initial seller of the items to be signed may stored. For example, if the item to be signed is a special item, such as an authentic jersey actually worn by a certain player, information about dealer or prior owner of this item may be recorded. Similarly, if, for example, the item to be signed is a limited edition item of memorabilia (such as a portrait of a player) generated by a manufacturer, additional information about the manufacturer and item might be recorded as well.

Once, information about the item(s) to be signed is recorded, an ID code is generated and assigned to each item and/or each inventory lot of the item(s) to be signed. This code may be generated from the master database 50. (Step 1010). As discussed above, the ID code may be generated in many forms but is preferably comprised of a unique, randomly generated number/character ID. In addition, an ID code may be assigned to each inventory lot of the items being signed instead of or as an additional step to assigning an ID code to each item.

The ID code assigned to each item and/or each inventory lot may be produced on a tamper evident label or attachment, such as a sticker or tag, and applied to the surface of each item 10 to be signed. (Step 1020). This code may also be applied to the item using infrared or ultraviolet activated ink. Alternatively, a separate additional code could be applied to the item using infrared or ultraviolet activated ink. The ID code(s) may then be stored and registered in the registration database 50.

After the ID codes are applied to the items to be signed, other components of the system for authenticating are implemented at the location of the particular sporting event or scheduled appearance where the signings will take place. These components may include first input device 40 to record or input other data associated the item being signed, second input device 30 to record or input at least one digital image associated with the item being signed, and processor 110 which may itself include the first input device 40. Processor 110 may comprise a personal computer, workstation, server or other component that maintains the necessary hardware and software to carry out the authenticating processes described herein. Processor 110 records and processes the at least one digital image and other data associated with the item being signed and may be configured to include registration database 50 and the components of server 100 discussed below. However, preferably registration database 50 and server 100 will be maintained separately by the authenticating service provider and/or other

third party service providers at remote locations. For example, registration database 50 may be maintained remotely by a separate division of the authenticating party attending the signing event in order to restrict access or maintained by an independent third party service provider to ensure that the integrity of the data stored in the registration database is not compromised. Similarly, server 100 which maintains or is connected to a secure time and date reference (discussed below) is also preferably maintained by a third party independent of the authenticating party attending the signing event to ensure that the integrity of data it receives and the time and date reference are not compromised. In addition, an output device 60 for generating a certificate of authenticity (COA), which may comprise a printer, is also connected to processor 110 and may be located at a remote or local location as well.

Processor 110 may be connected to registration database 50, server 100, and/or the output device 60 by any number of methods including by Internet connection, a direct dial-in connection, a modem connection, facsimile transmission, e-mail connection, wireless connection, links through dedicated computer connections, dedicated hardwire connections or any other methods for connecting to a computer server or uploading digital files or other information as are known in the art.

Once the local components of the system for authenticating memorabilia are implemented at the site of the sporting event or scheduled appearance, the item to be authenticated is signed by the athlete or other personality and eye-witnessed by a trained representative of the authenticating service provider. (Step 1030). It should be understood, however, that embodiments of the present invention are not limited to authenticating sports memorabilia but may be employed by the authenticating service provider in other areas such as for book signings, celebrity gatherings and other events where an item is to be authenticated.

At or around the time of signing, pertinent information concerning the signed item is entered and recorded by processor 110. (Step 1040). Such information may include the name of the athlete or personality signing the item, the owner's information, a description of the item being signed, the name of the witness, city and date of authentication, and the ID code. This information may be recorded or entered by the witness himself or another representative of the authenticating service provider or may be prepared in advance and released or recorded by processor 110 upon completion of the event or each time the item is signed where the pertinent information in known in advance of the actual signing. Some or all of this information may be stored locally by the authenticating service provider and/or stored in the registration database.

In addition, at least one digital camera and/or at least one digital video recorder 30 is provided to record at least one digital image of the signed item. (Step 1050). In a preferred embodiment, the digital camera or digital video recorder 30 will record both a digital image of the actual signature of the item that was signed and a digital image of the athlete or personality signing the item at the event location. The digital camera or digital video recorder can be operated by the witness or another representative or set to record digital images automatically throughout the signing. It is also possible to employ other input devices to record the digital image of the signed item. For example, where the signed item is a paper item or other flat item such as a photograph, a scanning device may be used to scan images of the signed item.

In a preferred embodiment the signature of the item and ID code are represented in a single digital image to ensure that the correct digital image is assigned to the authenticated item. The second input device 30 or other image recording device is adapted to create digital images to be input to processor 110 and stored.

To perform the step of time and date stamping each digital image, processor 110 is preferably connected to a digital file authentication system such as server 100 which can determine the time an digital image was first received from processor 110. Server 100 operates in one aspect by recording additional independent data which is stored with each digital image. (Step 1060). In one embodiment, this additional data includes a "true date" which is gleaned from a secure clock (described in further detail below) which is not settable by the user (the Authentidate); a number that may be derived from a cyclic redundancy code (CRC) algorithm (described in further detail below) against the image data, this number is called the "image CRC"; and a CRC derived from the "true date", called the "date CRC".

This additional data is preferably recorded within each digital image as soon as possible after the image is acquired from processor 110. As will be discussed in further detail, if the image is altered in any way after the recording of the additional data, recalculation of the image CRC on the altered image will not match the original CRC recorded within it. Thus, the fact that the image has been altered or is otherwise compromised can be detected. Likewise, if the true date is altered in any way, recalculation of the date CRC will similarly reveal this fact. Thus, the server 100 provides a method for ensuring that the image associated with each item being signed (e.g. the autograph) was recorded on the specified date and has not been altered in any way since.

Once the one or more digital images associated with the signed item and the pertinent information have been input and/or recorded in processor 110 and the one or more digital images sent to the digital file authentication system such as server 100, the owner or purchaser of the signed item is registered in a registration database 50 of the authenticator or other third party service provider. The registration database 50 may be organized by ID code to verify ownership and track ownership history (Step 1070). At this time a Certificate of Authenticity (COA) may also be generated and provided to the owner of the signed item.

(Step 1080). The COA may also be stored electronically, for example, in the registration database 50. As shown in Figure 3, a sample COA is illustrated which includes pertinent information concerning the signed item such as the name and address of the owner of the signed item, the name of the athlete or personality signing the item, the name of the witness, the date and city of the authentication, the AG code, a digital image of the signature of the item, and a digital image of the athlete or personality signing the item. Other details, such as the company providing the item of memorabilia, a description of the item and the item number within the series may also be provided. The COA may be presented to the owner in the form of a digital file, a paper certificate or a plastic ID card. In addition, the owner may be provided with digital access to the information embedded in the COA or other item details through a web site maintained by the authenticating service provider.

In a preferred embodiment, owner information, including the ID code is stored on a registration database 50 of the authenticating party or other third party service provider. Whenever the item is sold to a subsequent buyer, the identity of the registered owner authenticity of the signed item can be verified. When the product changes hands, the new owner obtains the Certificate of Authenticity from the prior owner. In order for the new owner to be registered, the old COA is sent to the service provider with updated owner information. At this time, the old certificate is destroyed and a new certificate is issued and the item is re-registered and the owner registration database is updated. As a further level of security, the party maintaining the registration database will only allow one COA to be in existence at any give time for any particular item. As yet a further level of security, the information embedded in each COA, a digital image of each COA itself, and/or other pertinent data or information concerning the item of memorabilia and the signing event may be sent to a digital file authentication system such as server 100 to be time and date stamped just as each digital image may be time and date stamped.

As discussed below, a preferred method for authenticating memorabilia of the present invention uses server 100 to provide secure date and time stamping of the digital image of the signed item. However, other methods of verifying the digital image of the signed item are possible. For example, in one system, a third party file registration service may be provided which allows the authenticating party (i.e. the party attending the signing event and recording the digital images of the signed item) to locally select a digital file (e.g., the digital image of the signed item or other data concerning the signed item) and to locally run a program provided by a service provider to create an "electronic signature" of the selected digital file based solely on file content. The signature along with a user-provided file name and user-selected keywords are uploaded to the provider's site and stored in a registration database maintained by the file registration service provider under an account established by the authenticator service provider.

Verification of content and submittal date of the digital file at a later time requires going on-line to access the service provider's site and retrieving the prior registration record by file name or keywords. The retrieved database record shows the file signature and the original date that the file signature was registered. To complete verification, the authenticating party must run (locally again) the electronic signature program on the file to be verified and compare the registered signature to the retrieved registered signature to determine whether the signature of the digital file in question matches that of the originally registered file. What the authenticating party now has is verification that the signature of the file in hand matches the signature of a file which was registered on a particular date. Other methods of verifying the content and creation date of the digital image of the signed item and other data associated with the signed item are possible such as having a separate division of the authenticating party or other third party service provider store and/or register the digital

image or a digital file containing information pertinent to the signed item in a secure storage device or database and logging the time and date the image was first created or submitted.

However, as shown in Figure 4 and described in further detail below, one advantageous method of authentication utilizes server 100 which includes or is connected to secure clock 130 to verify and authenticate image files associated with the item being signed. As shown in Figure 4, a server 100 is configured in communication with processor 110 of the authenticating system, storage device 120 and a secure time and date reference 130. In this embodiment, the secure time and date reference 130 is provided by a hardware device or service provider which incorporates a secure clock.

Original images associated with the signed item will be obtained from processor 110. The resulting digital image will be processed by server 100 as discussed in further detail herein, and may be stored on storage device 120 from where it can be later retrieved.

A digital file authentication system such as server 100 operates in one aspect by recording additional independent data with each stored digital image. In one embodiment described in further detail below, these additional data include: a "true date" which is gleaned from a secure clock (described in further detail below) which is not settable by the user (the Authentidate™); a number derived from a cyclic redundancy code (CRC) algorithm (described in further detail below) against the image data, this number is called the "image CRC"; and a CRC derived from the "true date", called the "date CRC".

These additional data are preferably recorded within each digital file as soon as possible after the image is acquired by the system. As will be discussed in further detail, if the image is altered in any way after the recording of the additional data, recalculation of the image CRC on the altered image will not match the original image CRC recorded within it. Thus, the fact that the image has been altered or is otherwise compromised can be detected.

Likewise, if the true date is altered in any way, recalculation of the date CRC will similarly reveal this fact.

The image and date CRCs can be checked and verified at any time. If the recalculated value matches the recorded value, it can be stated with extreme confidence that the image presently recorded was recorded on the specified date and has not been altered in any way since then. No other known system, including paper storage, can offer similar assurance as to the creation date or authenticity of a document.

With reference to Figure 5, the operation of one example of a digital file authentication system which may be utilized in the present invention will now be described. Digital files (such as an image of the signed item, a digital Certification of Authentication, or other files containing pertinent information about the signed item) are first acquired (either retrieved from storage or received from input device 110). (Step 200.) Date and time information is obtained from secure clock 130 (Step 202) or may be requested from a third party timestamp service. The secure clock 130 is preferably maintained by another independent service provider which supplies a secure, accurate and reliable time and date which is not easily compromised. However, as discussed below, secure clock 130 may be maintained and the timestamp function performed by the party operating server 100.

Proper operation of the secure clock or timestamp service provided is assessed. (Step 204.) If the secure clock is deemed functional, then the date and time data are accepted as read from the clock (in step 202). If a failure of the secure clock is determined, an error indication will be returned and the image processing is halted. (Step 206.) With the clock having been deemed functional (in step 204), special tags (as will be discussed infra) and the Authentidate information (including date and time) are added to the digital file and the CRC data fields are initialized to 0 (i.e., the data fields are filled with 0's). (Step 208.)

Two computed values are then calculated, which are derived from the image content and Authentidate information, respectively. The computed values can be computed in any fashion based on data contained within the digital file which will allow detection of data corruption, such as for example, a standard checksum. In this embodiment of the present invention, cyclic redundancy codes ("CRCs"), essentially a more complex checksum calculation, are used to derive the computed values. Any calculation method, however, is acceptable which will provide a number which is derived from the document content data and is suitable for detection of data corruption.

In this embodiment, the computed values are generated by a known CRC algorithm (which will be discussed in further detail below) which is run on both the image content and the Authentidate, creating an Image CRC and an Authentidate CRC, respectively. (Steps 210, 212.) The Image CRC and Authentidate CRC are "transformed" by a proprietary mathematical transformation for added security (as will be discussed infra) creating an Image CRC' and an Authentidate CRC'. (Step 214.)

The image file is then marked with the Image CRC' and Authentidate CRC'. (Step 216.) The marked digital files are stored on media by storage device 120. (Step 218.) The authenticity of the image and the time and date stamp can then subsequently be determined by examining the computed values stored within the Digital Files as shown in Fig. 6 which depicts an exemplary flow chart describing one embodiment for validating CRCs in a filed image.

The first step in validating the CRCs in a digital file is to read the special tag and date areas and retrieve the stored image CRC and date CRC values. (Step 300.) If the CRC values cannot be located or read in the digital file (step 302), then it is determined that either the image has not been properly filed or the image has been altered or is otherwise compromised, and an error is posted. (Step 304.) If the special tags are found, the CRCs are

recalculated for the digital file and the date string. (Step 306.) The same algorithms used to calculate the CRCs initially are used to regenerate them at this point. The recalculated image CRC is transformed and compared to the image CRC read from the tag. (Step 308.) (Alternatively, the stored image CRC can be reverse transformed prior to comparison to the recalculated value.) If the recalculated digital file CRC does not match the one stored in the special tag, the image is determined to have been altered or otherwise be corrupted and an error is indicated. (Step 310.) If the stored and recalculated image CRCs compare favorably (i.e., they match), the date CRCs are tested. The recalculated date CRC is transformed and compared to the date CRC read from the tag. (Step 312.) (Alternatively, the stored date CRC can be reverse transformed prior to comparison with the recalculated value.) If the recalculated date CRC does not match the one stored in the special tag, the date string is determined to have been altered or be otherwise corrupted and an error is indicated. (Step 314.) If the date CRCs match, at this point both image and date CRCs have compared favorably, the digital file is determined to be unaltered and thus authenticated. (Step 316.) It should be appreciated that the incorporation of the CRC in the image may use alternative methods, such as digital watermarking in which digital watermarks are integrated within digital files as noise, or random information that already exists in the file, thereby making the detection and removal of the watermark difficult.

As will be appreciated from the foregoing description, the use of a secure, non-compromisable clock serves as a secure time and date source which is not alterable by the user. The secure clock 130 is preferably maintained by an independent service provider other than the authenticating party and other than the service provider operating server 100 in order to supply a secure, accurate and reliable time and date information which is not easily compromised. However, it is also possible that secure clock 130 may be maintained by the party operating server 100. In this case, one could use either custom designed hardware or a

commercially available product that offers a secure clock. In either case, a mechanism must be in place to prevent fraudulent or arbitrary date/time adjustment. One embodiment in which the operator of server 100 could supply the secure clock itself is described in U.S. Patent Application 09/562,735, pp. 11-15, which is hereby incorporated by reference.

The computed values mentioned above with reference to Figure 5 in the present invention are Cyclic Redundancy Codes (CRCs). The CRC is a 32 bit-integer value which represents the result of performing the known CRC-32 algorithm on a block of data. The CRC-32 algorithm is a common, public domain algorithm for detecting even minute changes in data with a variety of applications. For example, CRCs are used in the communications field to verify that data has been transmitted correctly over transmission lines of unknown quality. It is also used to detect corruption of compressed data such as in the popular PKZIP utility. One of the strengths of CRCs is detecting changes to data which might otherwise go undetected. For example, if bit errors occur in a given block of data but their sum is coincidentally the same as that of the original data, this error might go undetected if a standard checksum were to be used. The CRC-32 algorithm would detect this type of change because the resulting code is not simply a sum of the component data as in a standard checksum.

A technical discussion of the CRC-32 algorithm will not be presented here. There are many sources of CRC-32 algorithms and source code in the public domain. As stated earlier, use of the CRC is not required for the present invention per se, and any calculation method is acceptable which will provide a number which is derived from the image data and is suitable for detection of data corruption.

While a CRC value alone may be used, a higher level of security can be incorporated into the present invention to ensure the authenticity of an image by addition of a mathematical transformation to the CRC value. As indicated, a typical algorithm to calculate

a CRC-32 is in the public domain and thus easily accessible. This fact, in conjunction with the details provided herein, would allow anyone to recalculate the CRC on an altered image, enabling them to counterfeit an "Authentidate" and falsely confirm the image as authentic and unaltered. In the present invention, the actual calculated (image or date) CRC is mathematically transformed to a new value prior to image marking. The functional requirements of the transformation are that the resultant value for any input value is consistent, and that the resultant value is unique for each unique input value. The transformation could, for example, be a permutation of the bit-order of the input, an exclusive OR of the input value with a consistent, predetermined "magic" number, or a combination of these operations.

While the particular transformation technique implemented is not critical, it should be understood that the specific technique used to accomplish the transformation in the practice of this invention should remain confidential to the provider, i.e., a "proprietary transformation technique", as any disclosure or dissemination of the method would likely compromise system security and effectiveness. To give a simple parallel, failure to safeguard the proprietary transformation technique would essentially be the equivalent of password protecting a file and then distributing the password.

Recording information in tags within digital files requires knowledge of the individual digital file formats and the standards governing the structure of their formats. These standards dictate how information will be stored in the file, in what order, using what compression algorithm, etc. Most digital file formats have provisions for accommodating storage of user data in the digital file in addition to the image data. A file management and imaging system embodiment of the present invention may use known TIFF (Tagged Image File) and JPEG (Joint Photographic Experts Group) file formats for storage of (scanned) bitonal and color images, respectively. The standards for TIFF and JPEG image file formats

allow for inclusion of user data inside the image file in a manner which does not affect the displayed image. As will be readily understood, the present invention is equally applicable to other file formats which have a mechanism to store user-defined data in the file or the file marked with the user-defined data can be stored in an ancillary file or separate database, for example, for word processing documents, spreadsheets, digitized audio or video or any other digitized file.

The known TIFF format is a file format which allows image data to be stored in a compressed manner along with information about the image (tags) such as compression method used, resolution, size, number of colors, title, date, etc.

A written world-wide standard defines the TIFF file format, what tags must be present, what tags are optional and how specific tags are used. The maintaining organization of the TIFF standard, Adobe Corporation, accepts requests for custom tag numbers for companies developing applications which use tags within the TIFF image. Adobe will assign unique numbers to individual companies to prevent interference between vendors. For example, an individual company may apply for and be assigned its own proprietary tags numbers, and other vendors will likewise be assigned their own unique proprietary tag numbers. Use of a custom tag allows storage of a custom data block. The TIFF specification calls for programs to ignore tags that they do not understand and which are not in the baseline specification. This allows common image viewers to view, display and print images which have custom tags because the image files still fit the TIFF specification.

In the case of TIFF image files, the following TIFF image tags are used:

Tag #	Use
10Dh	Document Name
10Eh	Image Description
132h	Date Time

9244h Custom Tag 1

custom data block contains proprietary information including:

Image CRC

Authentidate CRC

Illustrated in Fig. 7 is an exemplary flow chart demonstrating calculation of an image CRC for a TIFF image file. The calculation of the image CRC for the TIFF image file calls for calculating a CRC-32 on a given block of data using a given 32-bit seed value. The initial seed value is set to –1. (Step 500.) The routine works through the format of the TIFF file based on the Image File Directory (IFD) for the file, calculating CRC-32 for each IFD entry and their associated data (step 502) passing results of the prior CRC-32 as the seed to the next (step 510) until all the IFD entries have been cycled through. (Step 506.)

All tags and data areas are processed except the following tags and data areas (step 508):

Tag #	Description
0x010d	TIFFTAG_DOCUMENTNAME
0x010e	TIFFTAG_IMAGEDESCRIPTION
0x0132	TIFFTAG_DATETIME
0x9244	TIFFTAG_DOCSTARTAG1

After processing all IFD entries for the file (step 506), the proprietary transformation method (as described above) is used to transform the resulting CRC value into a unique and secure value CRC'. (Step 512.) The transformed image CRC value, CRC' is then stored in the image file. (Step 514.)

Illustrated in Fig. 8 is an exemplary flow chart demonstrating calculation of a date CRC for a TIFF image file. The calculation of the date CRC for the TIFF image file requires a routine which can calculate a CRC-32 on a given block of data using a given 32-bit seed

value. The initial seed value is set to the image CRC value. (Step 600.) The routine reads the 0x0132 TIFFTAG_DATETIME tag. (Step 602.) If the DATETIME tag cannot be found and read (step 604), an error is returned (step 605), otherwise, a CRC-32 is calculated for the data contained within the DATETIME tag. (Step 606.) The resulting CRC is then transformed into CRC' by means of the proprietary transformation technique (step 608) and stored within the image file. (Step 610.)

The Joint Photographic Experts Group developed the namesake format and maintains the standard for JPEG and the JPG file format (sometimes also called JFIF – JPEG File Image Format). This format was developed for the storage and transmission of photographic images. The compression techniques used are ideally suited to storing subtle differences between color changes, such as a photograph.

As is known, a JPG file is interpreted as a stream of characters with special identifiers called "markers" separating different elements of the image information and image data. The exact meaning of each marker is not important to this discussion except that the JPG standard defines a set of markers to be used by manufacturers for special or proprietary features. These markers are named "APPx" where x is a digit between 0 and 9 inclusive.

The present invention adds a special marker and data block to JPG files when they are stored. In this embodiment, the "APP8" marker will be used for the simple reason that this marker is rarely used by other manufacturers. This marker holds various proprietary information including the following:

Authentidate

Image CRC

Authentidate CRC

Illustrated in Fig. 9 is an exemplary flow chart demonstrating calculation of an image CRC for a JPEG image file. The calculation of the CRC for the JPEG image file requires a

routine which can calculate a CRC-32 on a given block of data using a given 32-bit seed value. The initial seed value is set to –1. (Step 700.) The image file data is read sequentially and the position of the APP8 is determined and read. (Step 702.) If the APP8 marker cannot be found and read (step 704), an error is returned. (Step 705.) A CRC-32 is calculated for all data in the file from the beginning of the file up to but not including the APP8 marker. (Step 706.) The result of this calculation is used as a seed to calculate a CRC-32 on the remainder of the file following the APP8 marker. (Step 708.) The resulting CRC is transformed into CRC' by means of the proprietary transformation technique. (Step 710.) The transformed image CRC' is then stored within the image file. (Step 712.)

Illustrated in Fig. 10 is an exemplary flow chart demonstrating calculation of a date CRCs for a JPEG image file. The calculation of the CRC for the JPEG image file requires a routine which can calculate a CRC-32 on a given block of data using a given 32-bit seed value. The initial seed value is set to the image CRC value. (Step 800.) The file is read sequentially and the position of the APP8 is determined and read. (Step 802.) If the APP8 marker cannot be found and read (step 804), an error is returned. (Step 805.) A CRC-32 is calculated for the secure data string within the APP8 data area or block. (Step 806.) The resulting CRC is transformed into CRC' by means of the proprietary transformation technique. (Step 808.) The transformed date CRC' is stored within the image file. (Step 810.)

The present invention has been illustrated and described with respect to specific embodiments thereof. It is to be understood, however, that the above-described embodiments are merely illustrative of the principles of the invention and are not intended to be exclusive embodiments. To facilitate discussion of the present invention, digital image files (e.g., of the signed item) are presumed to be input to the server 100 in one embodiment of the present invention. However, it should be understood by one skilled in the art, that the server 100 will

be equally applicable to any digital file regardless of its source or how it is generated. For example, the server 100 may receive and time and date stamp other digital files containing other information pertaining to the signed item such as the ID code, witness and owner information, an electronic certificate of authenticity and other data concerning the signed item.

Moreover, it should be understood that server 100 need not mark and store each digital file in order to perform the digital file authentication. In one embodiment of the present invention, server 100 receives a digital file (such as an image of the signed item), retrieves a time stamp to note the time of receipt of the file, and performs the step of obtaining the digital signature of the document. The time stamp and the digital signature, along with other information that may be desirable, such as a file ID number, user identification information, or other parameters to identify the file may be stored in a database maintained by the operator of server 100. Server 100 may also rend a receipt to the user (e.g. the party authenticating the item of memorabilia, the owner, or the party maintaining the registration database) which includes pertinent information relating to the submitted file, including, for example, the time stamp, the digital signature, the file ID number, or other information. In one embodiment, a digital copy of the submitted file may be maintained by server 100. The file could be saved in association with the log of information to be kept on the file such as the ID number, the time stamp and the digital signature. Alternatively, the digital file is not saved nor maintained by the operator of the server 100. After the file has been processed in order to derive its digital signature, the digital file may be returned or deleted. For this alternative, a digital copy of the file is not maintained at the site of the operator of server 100 performing the date and time stamp service and the user (e.g., the authenticating party that witnessed the signing or the operator of the registration database) is responsible for maintaining a digital copy of the file. In the future, the user or any third

party, such as the owner of the item or operator of the registration database 50, can verify if the newly submitted file is the same as the document originally submitted by the user, and further can verify the date upon which the original file was originally submitted.

To verify whether a digital copy of a file, such as an electronic certificate of authenticity, is the same as the original document submitted by the user on the date and time recorded in the log, the server 100 runs the digital signature routine on the file to be verified. This second digital signature is compared against the original digital signature, and if they are the same, then the server 100 may issue notice that digital file is verfied. Other methods of digital file authentication and digital file signature and time stamp creation and verification are described in United States patent application 09/729,411 which is hereby incorporated by reference.

Alternative embodiments capturing variations in the enumerated embodiments disclosed herein can be implemented to achieve the benefits of the present invention. It should further be understood that the foregoing and many various modifications, omissions and additions may be devised by one skilled in the art without departing from the spirit and scope of the invention. It is therefore intended that the present invention is not limited to the disclosed embodiments but should be defined in accordance with the claims which follow.

What is claimed is:

1. A method of authenticating memorabilia, the method comprising the steps of:

applying an identification code to an item of memorabilia

recording a digital image of the item of memorabilia

providing date and time information from a secure date and time reference;

generating a date/time value derived from said date and time reference;

generating an image value derived from said digital image;

marking said digital image with said date and time information, said date/time value and said image value; and

storing said marked digital image.

2. The method according to claim 1, further comprising the step of assigning an owner to the item of memorabilia wherein the owner of the item of memorabilia and the identification code are recorded in a database.

3. A method of authenticating memorabilia comprising the steps of:

applying an identification code to an item of memorabilia;

obtaining a handwritten signature on the item of memorabilia from a signor;

recording a digital image of the item of memorabilia;

providing date and time information from a secure date and time reference;

generating a date/time value derived from said date and time reference;

generating an image value derived from said digital image;

marking said digital image with said date and time information, said date/time value and said image value; and

storing said marked digital image.

4. The method of claim 3 wherein a witness observes the step of obtaining a handwritten signature on the item of memorabilia.

5. The method of claim 4 further comprising the step of obtaining a second digital image of the signor.

6. The method according to claim 5, further comprising the step of assigning an owner to the item of memorabilia wherein a name of the owner of the item of memorabilia and the identification code are recorded in a database.

7. The method according to claim 6, further comprising the step of generating a certificate of authenticity, said certificate of authenticity including the name of the owner of the item of memorabilia, the identification code, and the digital image of the item of memorabilia.

8. A method of authenticating memorabilia comprising the steps of:

applying an identification code to an item of memorabilia;

obtaining a handwritten signature on the item of memorabilia from a signor;

recording a digital image of the item of memorabilia;

performing a digital signature routine on the digital image to obtain a digital signature of said digital image;

creating a time stamp corresponding to the time of submission of said digital image; and

storing said digital signature and said time stamp.

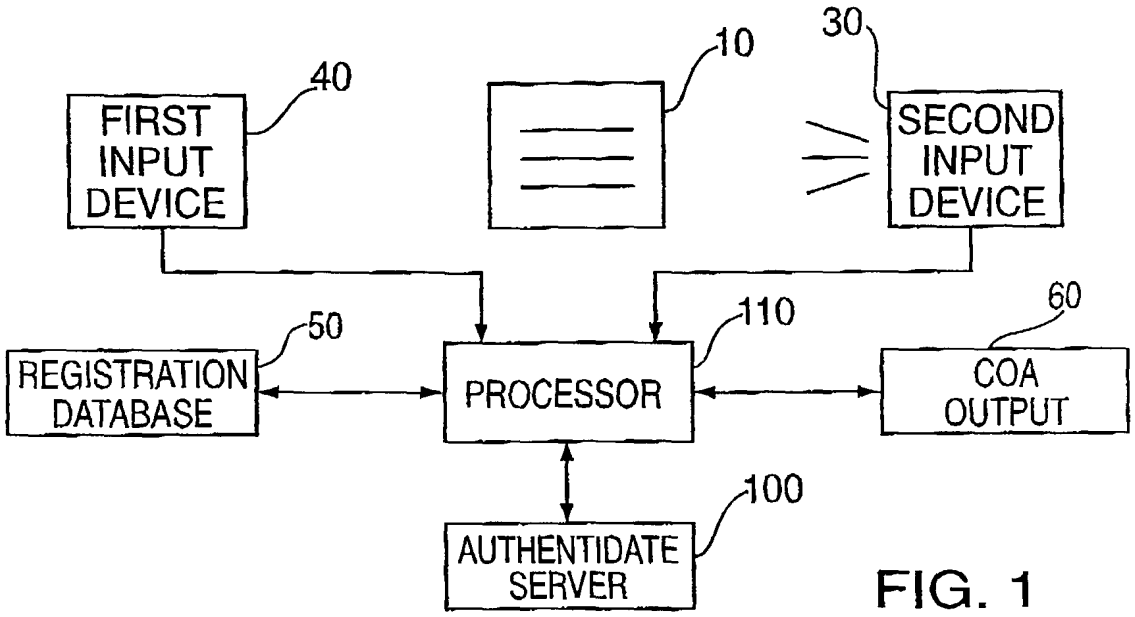

10
30
40
FIRST INPUT DEVICE
SECOND INPUT DEVICE
50
110
60
REGISTRATION DATABASE
PROCESSOR
COA OUTPUT
100
AUTHENTIDATE SERVER

FIG. 1

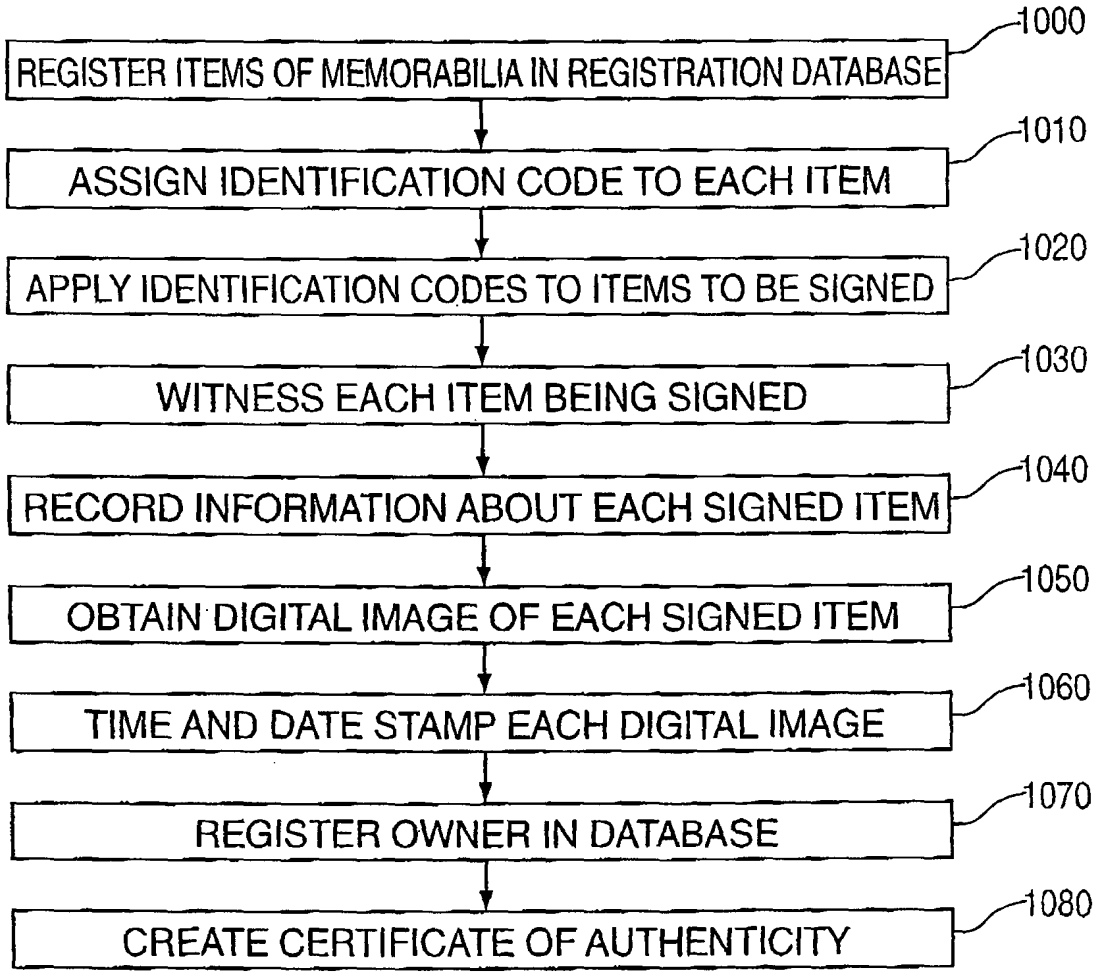

1000
REGISTER ITEMS OF MEMORABILIA IN REGISTRATION DATABASE
1010
ASSIGN IDENTIFICATION CODE TO EACH ITEM
1020
APPLY IDENTIFICATION CODES TO ITEMS TO BE SIGNED
1030
WITNESS EACH ITEM BEING SIGNED
1040
RECORD INFORMATION ABOUT EACH SIGNED ITEM
1050
OBTAIN DIGITAL IMAGE OF EACH SIGNED ITEM
1060
TIME AND DATE STAMP EACH DIGITAL IMAGE
1070
REGISTER OWNER IN DATABASE
1080
CREATE CERTIFICATE OF AUTHENTICITY

FIG. 2

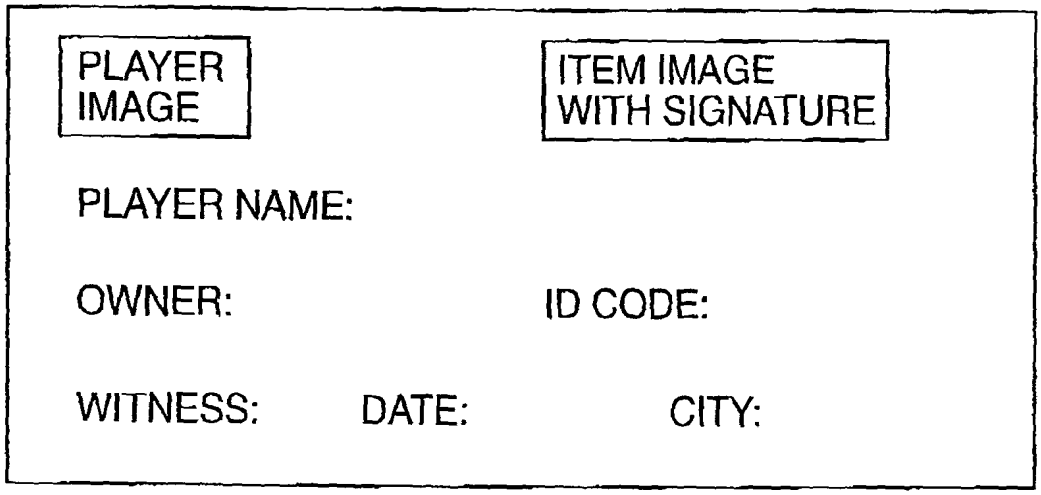

PLAYER IMAGE
ITEM IMAGE WITH SIGNATURE
PLAYER NAME:
OWNER:
ID CODE:
WITNESS:
DATE:
CITY:

FIG. 3

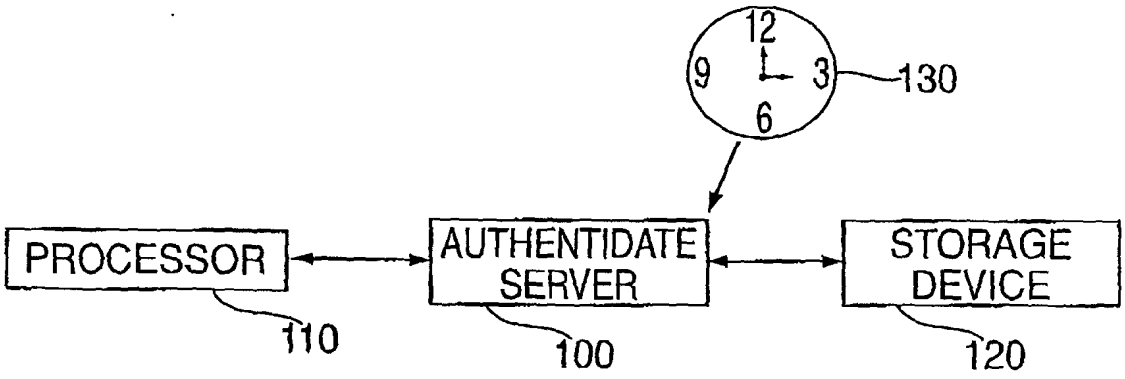

12
9
3
6
130
PROCESSOR
AUTHENTIDATE SERVER
STORAGE DEVICE
110
100
120

FIG. 4

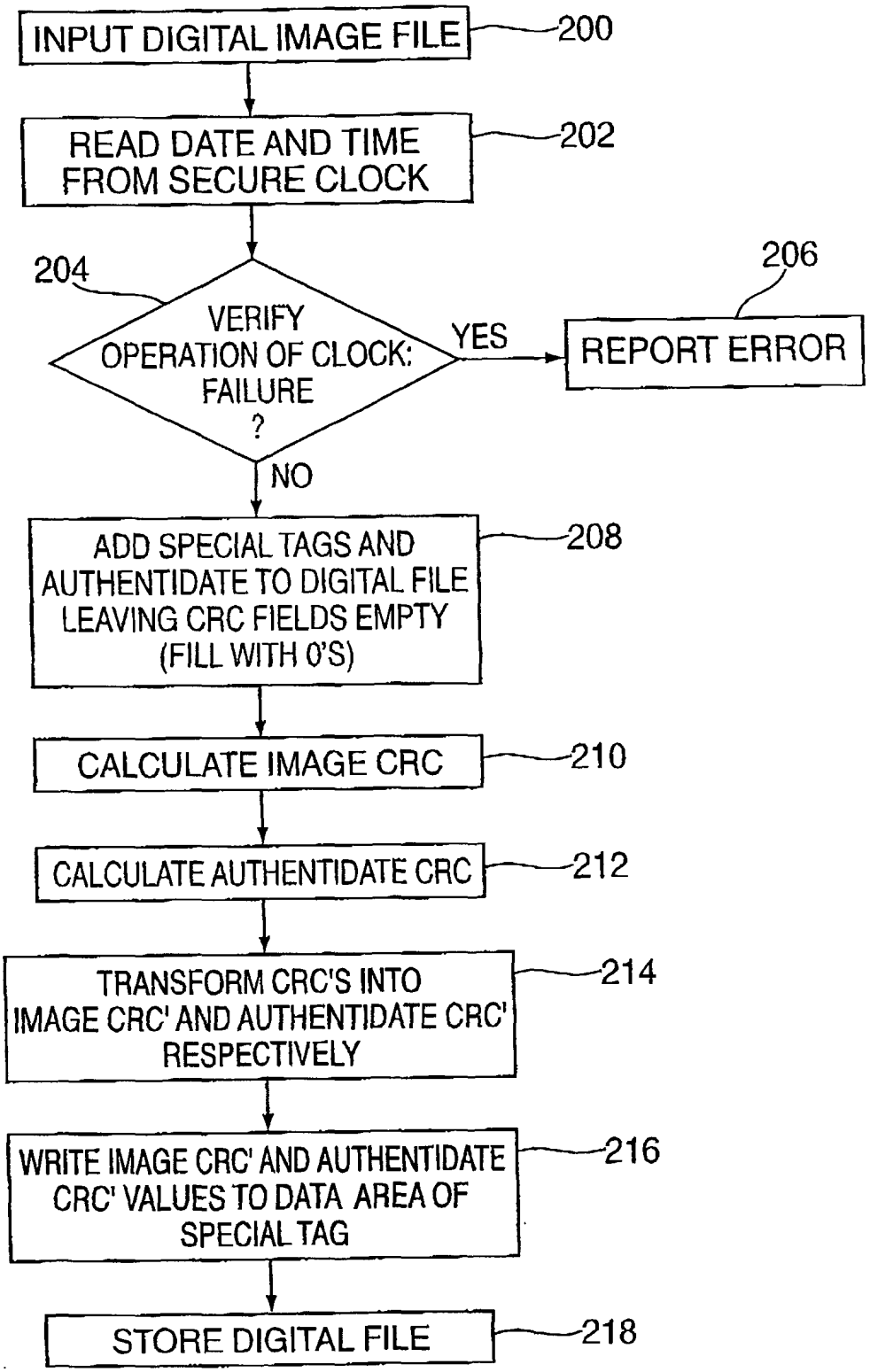

INPUT DIGITAL IMAGE FILE
200
READ DATE AND TIME FROM SECURE CLOCK
202
204
VERIFY OPERATION OF CLOCK: FAILURE ?
YES
206
REPORT ERROR
NO
ADD SPECIAL TAGS AND AUTHENTIDATE TO DIGITAL FILE LEAVING CRC FIELDS EMPTY (FILL WITH 0'S)
208
CALCULATE IMAGE CRC
210
CALCULATE AUTHENTIDATE CRC
212
TRANSFORM CRC'S INTO IMAGE CRC' AND AUTHENTIDATE CRC' RESPECTIVELY
214
WRITE IMAGE CRC' AND AUTHENTIDATE CRC' VALUES TO DATA AREA OF SPECIAL TAG
216
STORE DIGITAL FILE
218

FIG. 5

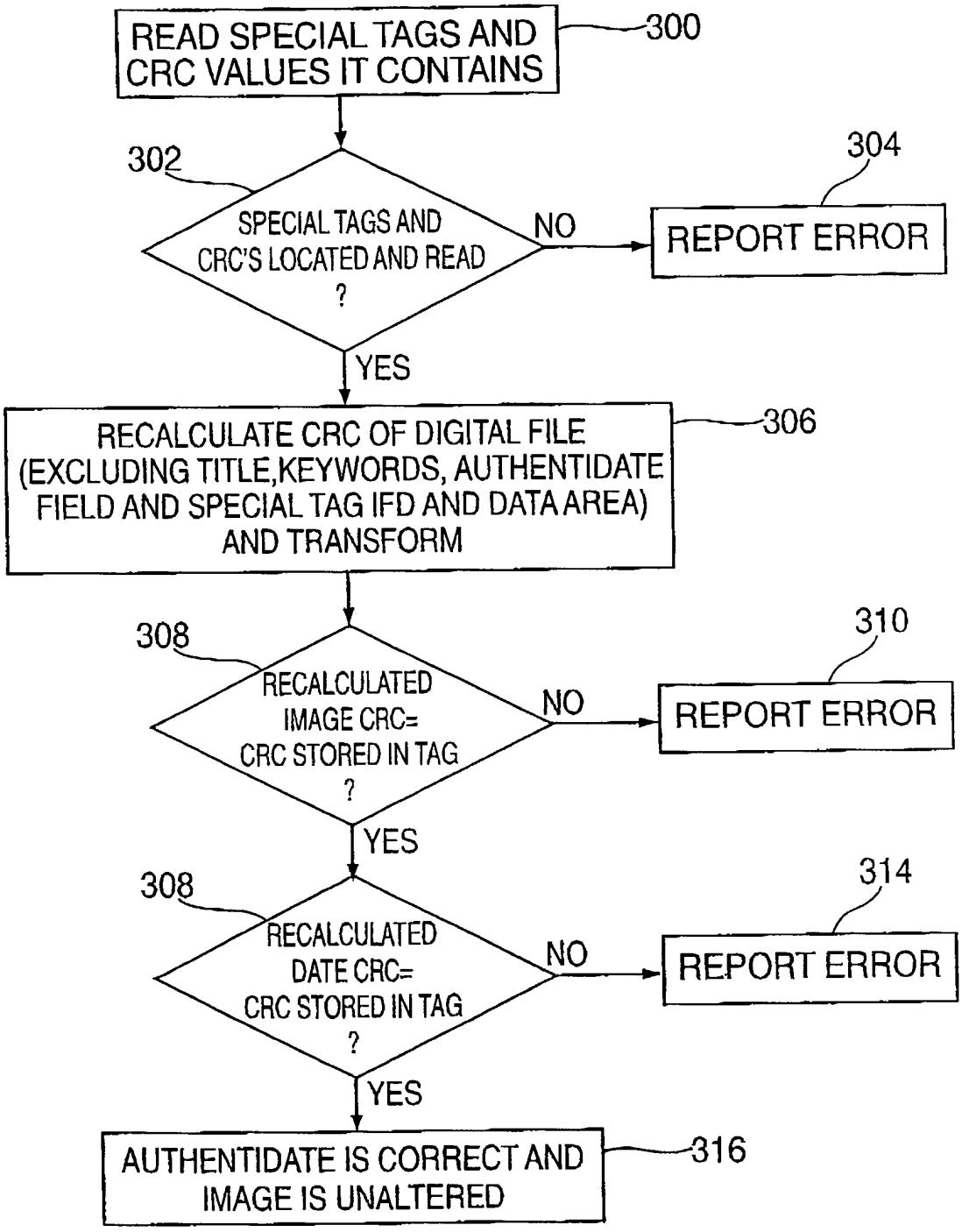

READ SPECIAL TAGS AND CRC VALUES IT CONTAINS
300
302
SPECIAL TAGS AND CRC'S LOCATED AND READ ?
NO
304
REPORT ERROR
YES
RECALCULATE CRC OF DIGITAL FILE (EXCLUDING TITLE,KEYWORDS, AUTHENTIDATE FIELD AND SPECIAL TAG IFD AND DATA AREA) AND TRANSFORM
306
308
RECALCULATED IMAGE CRC= CRC STORED IN TAG ?
NO
310
REPORT ERROR
YES
308
RECALCULATED DATE CRC= CRC STORED IN TAG ?
NO
314
REPORT ERROR
YES
AUTHENTIDATE IS CORRECT AND IMAGE IS UNALTERED
316

FIG. 6

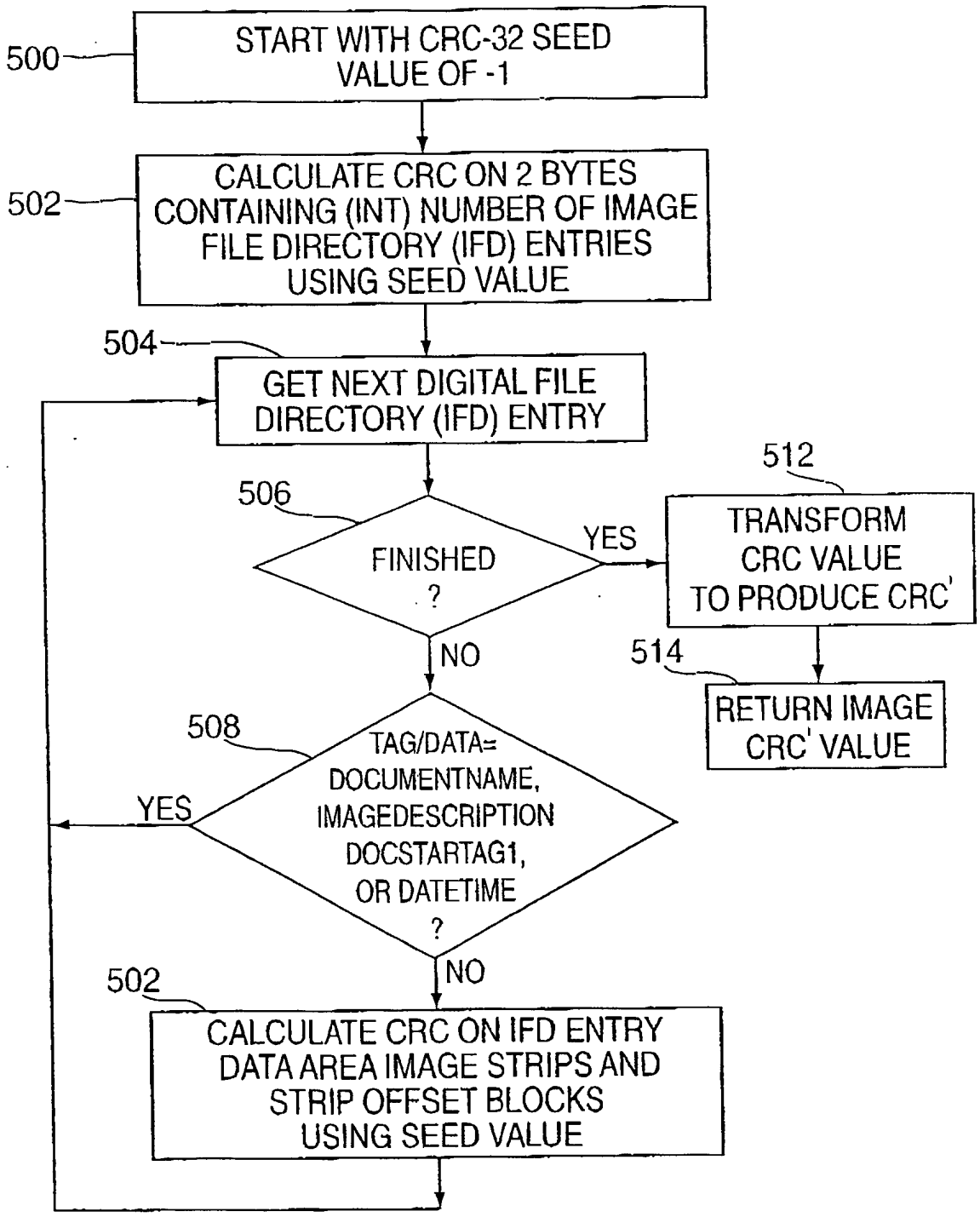

500
START WITH CRC-32 SEED VALUE OF -1
502
CALCULATE CRC ON 2 BYTES CONTAINING (INT) NUMBER OF IMAGE FILE DIRECTORY (IFD) ENTRIES USING SEED VALUE
504
GET NEXT DIGITAL FILE DIRECTORY (IFD) ENTRY
506
FINISHED ?
YES
512
TRANSFORM CRC VALUE TO PRODUCE CRC'
514
RETURN IMAGE CRC' VALUE
NO
508
TAG/DATA= DOCUMENTNAME, IMAGEDESCRIPTION DOCSTARTAG1, OR DATETIME ?
YES
NO
502
CALCULATE CRC ON IFD ENTRY DATA AREA IMAGE STRIPS AND STRIP OFFSET BLOCKS USING SEED VALUE

FIG. 7

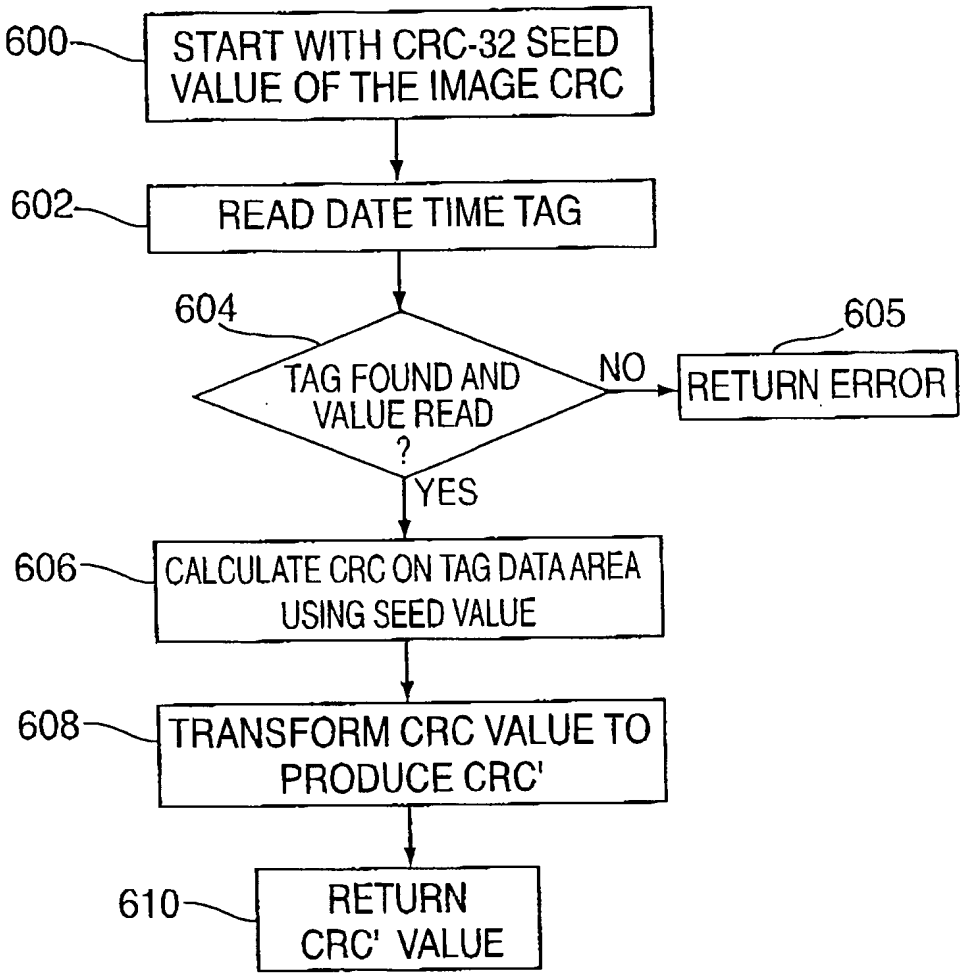

600
START WITH CRC-32 SEED VALUE OF THE IMAGE CRC
602
READ DATE TIME TAG
604
TAG FOUND AND VALUE READ ?
NO
605
RETURN ERROR
YES
606
CALCULATE CRC ON TAG DATA AREA USING SEED VALUE
608
TRANSFORM CRC VALUE TO PRODUCE CRC'
610
RETURN CRC' VALUE

FIG. 8

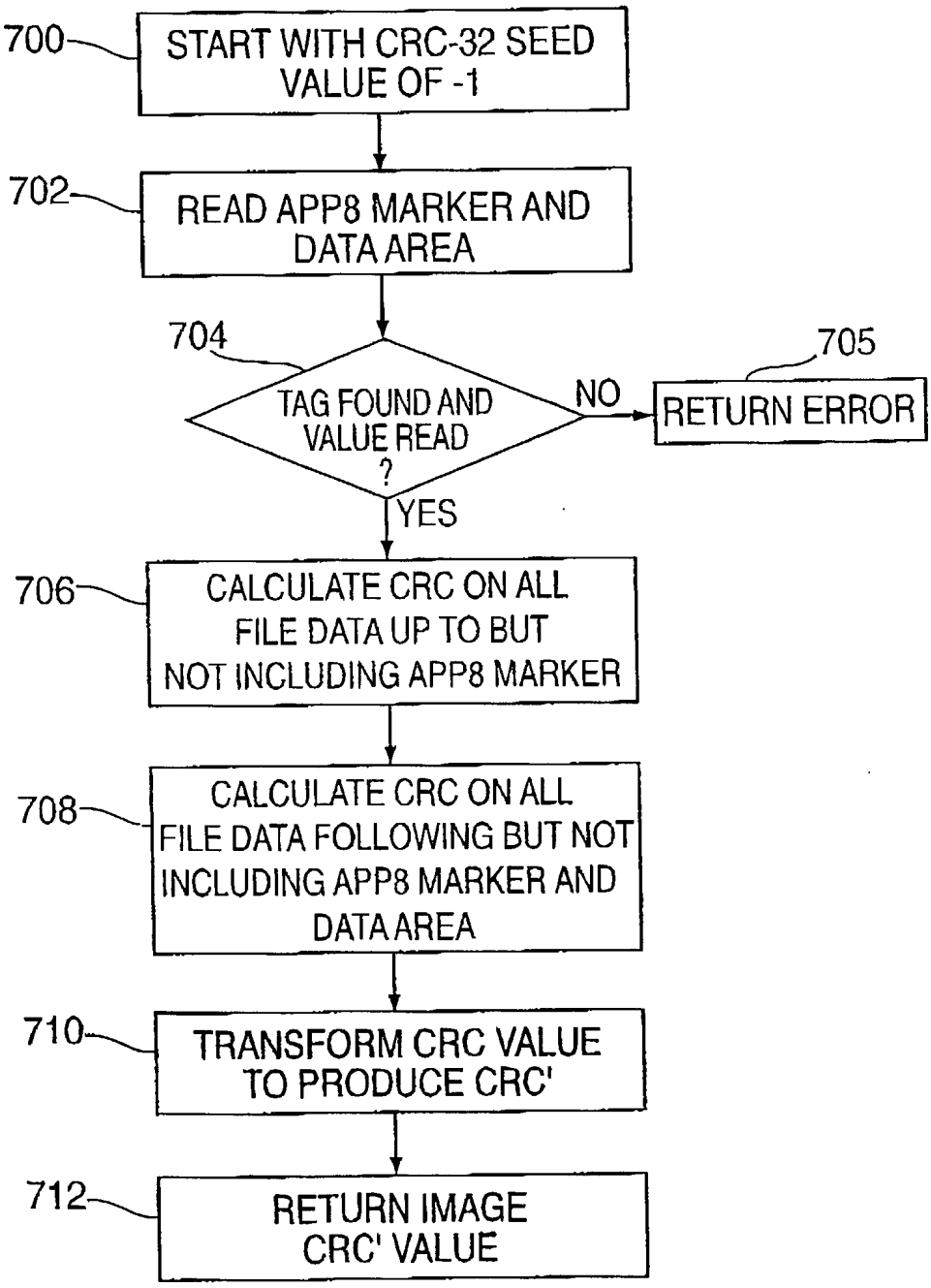

700
START WITH CRC-32 SEED VALUE OF -1
702
READ APP8 MARKER AND DATA AREA
704
TAG FOUND AND VALUE READ ?
NO
705
RETURN ERROR
YES
706
CALCULATE CRC ON ALL FILE DATA UP TO BUT NOT INCLUDING APP8 MARKER
708
CALCULATE CRC ON ALL FILE DATA FOLLOWING BUT NOT INCLUDING APP8 MARKER AND DATA AREA
710
TRANSFORM CRC VALUE TO PRODUCE CRC'
712
RETURN IMAGE CRC' VALUE

FIG. 9

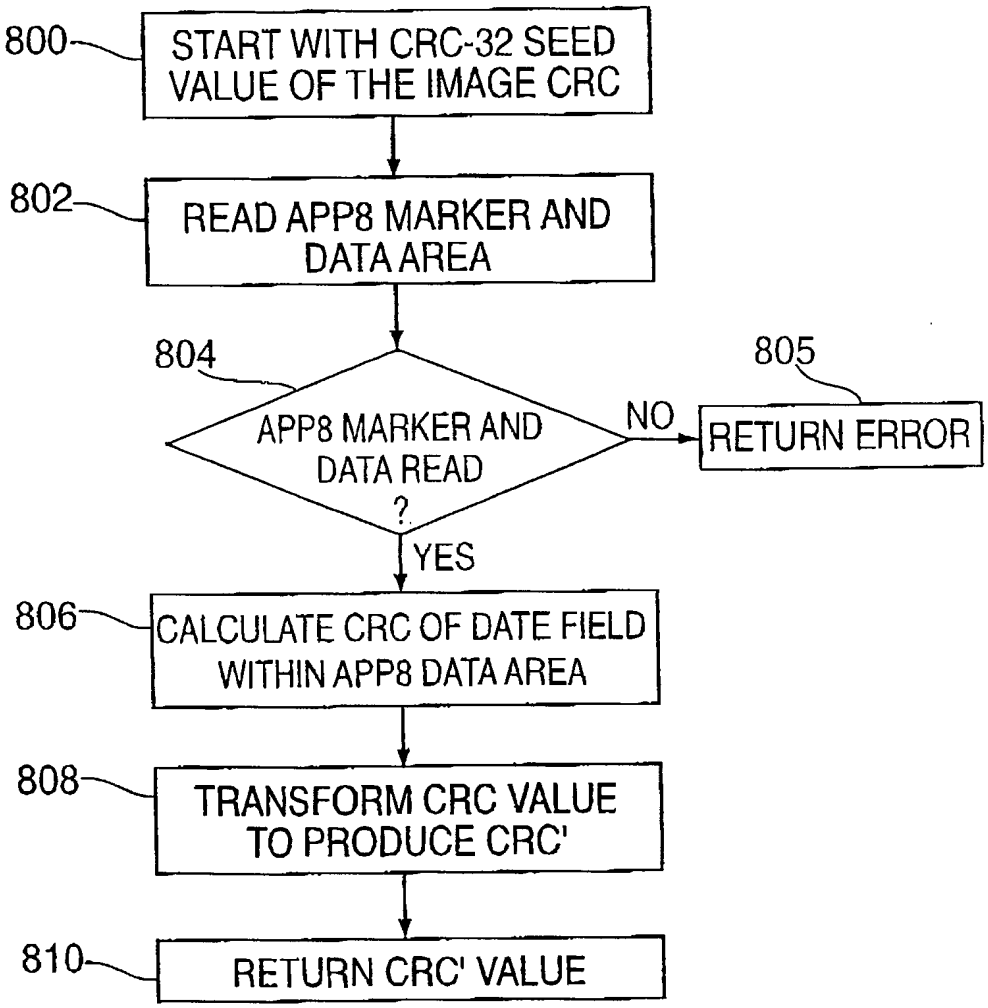

800
START WITH CRC-32 SEED VALUE OF THE IMAGE CRC
802
READ APP8 MARKER AND DATA AREA
804
APP8 MARKER AND DATA READ ?
NO
805
RETURN ERROR
YES
806
CALCULATE CRC OF DATE FIELD WITHIN APP8 DATA AREA
808
TRANSFORM CRC VALUE TO PRODUCE CRC'
810
RETURN CRC' VALUE

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/20697

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : Ho4L9/00
US CL : 713/178
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/178, 705/87

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East: autograph and protection and timestamp

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,250,549 B1 (DEFABIO et al) 26 June 2001, col. 7 lines 61-65, col 6 lines 20-30, col 4, lines 15-20; col 7, lines 54-65.	1-8
Y	US 5,923,763 (WALKER et al) 13, July 1999, col 11, lines 34-62.	1-8
Y, P	PUB 2001/0033676 A1 (NOYES) 25 October 2001, page 3 lines 11-33.	4
Y, P	US PUB 2002/0009033 A1 (CHRISTENSEN) 24 January 2002, page 5 par. 65.	1, 3
Y	Schneier, Bruce Applied Cryptography 2nd ed. 1996 pages 34-43.	8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2002 (30.09.2002)	23 DEC 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Nilesh Shah Telephone No. 703-305-8105

Form PCT/ISA/210 (second sheet) (July 1998)